								Page 1	of 2	
Form PTO-1449		U.S. DEPARTMENT OF COMMERCE		ATTY. DOCKET NO.		SERIAL NO.				
(MODIFIED)		PATENT AND TRADEMARK OFFICE			068398-010	09/761,771				
			APPLICANT							
INFORMATION DISCLOSURE CITATION				Virg	il D. Glig	or et al	· 1			
					FILING DATE GROUP ART LINITY				<b>`</b>	
_	(Use se	everal sheets if neces	ssary)		01/18/200	Mnassigned				
			U.S. PA	TEN	T DOCUMENTS	May of the				
EXAMINER		DOCUMENT				CLASS	SUB-	FILING DATE IF APPROPRIATE		
INITIAL	REF	NUMBER	DATE		NAME		CLASS			
PE	~						-	AFROFRIATE		
FOREIGN PATENT DOCUMENTS										
JUL 1 70		DOCUMENT	DOCUMENT				SUB-	TRANS	TRANSLATION	
70r	REF	NUMBER	DATE		COUNTRY	CLASS	CLASS	YES	NO	
TENT & TRADE	ME									
		OTHER DOCU	MENTS (Includii	ng A	uthor, Title, Date, Perti	nent Pages,	Etc.)	- " "		
	A1 /	A.J. Menezes et al, "Hash Functions and Data Integrity", Handbook of Applied Crytography, Chp 7, pp 223-								
		282; Chp 9, pp 321-383, 1997; CRC Press, Boca Raton								
	A2	Gligor et al, "Object Migration and Authentication", IEEE Transactions on Software Engineering SE-5, vol. 5,								
<i>V</i> )		pp. 607-611, 1979, IEEE								
27	А3	NBS FIPS Pub 46, titled "Data Encryption Standard", National Bureau of Standards, U.S. Dept of Commerce								
		January 1977, pp. 1-18								
n	A4	NBS FIPS Pub 81, Titled "DES Modes of Operation", National Bureau of Standards, U.S. Dept of Commerce								
		pp. 1-17, December 1980								
n	<b>A5</b>	Meyer et al, Cryptography; A New Dimension in Computer Data Security", A Guide For The Design and								
		Implementation of Secure Systems, pp. 69-71, 1982, John Wiley & Sons, 2 <sup>nd</sup> printing								
n	A6	Bellare et al, "A Concrete Security Treatment of Symmetric Encryption", Proceedings of the 38th Symposium								
		on Foundations of Computer Science, IEEE, 1997, pp. 394-403								
m n	A7	C.M. Campbell, "Design and Specification of Cryptographic Capabilities", in Computer Science And The Data								
		Encryption Standard, (D.K. Brandstad (ed.) National Bureau of Standards Special Publications 500-527								
n		U. S. Dept of Commerce, February 1978, pp. 54-66								
n	A8	Naor et al, "From Unpredictability to Indistinguishability: A Simple Construction of Pseudo-Random Functions								
- 1		From MACs", in Advances in Cryptolog – CRYPTO '98 (LNCS 1462), pp. 267-282, 1998, Springer-Verlag								
n.	A9	Goldwasser et al, "Lecture Notes on Cryptography", 1999, Available at								
- '		http://www.cse.ucsd.edu/users/mihir/papers/gb.pdf								
		Kohl et al, RFC 1510, The Kerberos Network Authentication Service (V5)", Internet Request For Comments								

EXAMINER DATE CONSIDERED

12/7/04

\* EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include any copy of this form with next communication to applicant.

July 17, 2001

1510

							Page 2	of 2		
Form PTO-1449 U.S. DEPARTME			NT OF COMMERCE	ATTY. DOCKET NO	SERIAL NO.					
(MODIFIED)		PATENT AND TRADEMARK OFFICE		068398-0	0102	09/761,771				
						<u>.</u>				
INFO	ORMATI	ON DISCLOSURE	CITATION	Virgil D. Gligor et al.						
				FILING DATE	GROUP ART UNIT					
]	(Use se	everal sheets if nece	ssary)	01/18/2	Unassigned					
		<u>-</u>	U.S. PATER	T DOCUMENTS						
EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB- CLASS	FILING DATE			
							APPROPRIATE			
PE JCP	<b></b>				·					
	FOREIGN PATENT DOCUMENTS  DOCUMENT  SUB- TRANSLATION									
111 1.7		DOCUMENT	DATE	COUNTRY	CLASS	SUB-	TRANSLATION			
30.	F	NUMBER	57.11.2			CLASS	YES	NO		
FORT & TRAC						<u> </u>				
OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)										
	A11	Petrank et al, "CBC MAC for Real-Time Data Sources:, Manuscript Available at								
n		http://www.cs.technion.ac.il/~erez/publications.html, 1999								
		Jueneman et al, "Message Authentication with Manipulation Detection Codes", Proc. Of the IEEE Symp. on								
A12 Security and Privacy, Oakland, CA, pp. 33-54, 1983, IEEE Computer Society										
<del></del>	A13	Stubblebine et al, "On Message Integrity in Cryptographic Protocols", Proceedings of the 1992 IEEE Computer								
2		Society Symposium on Research in Security and Privacy, pp. 85-104, 1992, IEEE Computer Society Press								
<del> </del>	A14	Kohl et al, "The use of Encryption in Kerberos for Network Authentication", Advances in Cryptology-CRYPTO								
n		1989, (LNCS 435), pp. 35-43, 1990, Digital Equip. Corp.								
	A15	D. E. Knuth, "The Art of Computer Programming – Volume 2: Seminumerical Algorithms", 1981, (2 <sup>nd</sup> ed.)								
3		Chapter 3, pp. 1-110, Addison-Wesley								
<del> </del>										
				<u>-</u>	Dr.	<b>^</b>				
		JUL 1 9 2001								
					JUL	1 9 2001				
		Technology Center 2100								
		Enter 2100								

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include any copy of this form with next communication to applicant.

DATE CONSIDERED

July 17, 2001

**EXAMINER** 

# 4

Form PTO-1449		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE			TTY. DOCKET N 068398	SERIAL NO. 09/761,771			
(MODIFIED) PATI		PATENT AND IN			PPLICANT	-0102	09/	761,77	
INFO	DRMAT	ION DISCLOSURE	CITATION	~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	V	rirgil D. Gli	gor et al	•	
			( , , , 3 <sup>18</sup>	in,   F	LING DATE		GROUP AR	T UNIT	
	(Use s	everal sheets if nece	ssark) WH	JAK C	01/18/	/2001		2131	
			CUAN PA	TENT	DOCUMENTS				
EXAMINER INITIAL	REF	DOCUMENT NUMBER	OCUMENT DATE			CLASS	SUB- CLASS	I IC	
						R			
						12	CEIVEL 16 7001		
						» NOV	1000	<b>&gt;</b>	
,,-						**Chnolog	enter 2100		
						1	enter 21		·
							100	1	
				-					
	ł. <u>.</u>	<u></u>	FOREIGN	PATEN	IT DOCUMENT	 'S	<u>.l</u>		
		DOCUMENT			· · · · · · · · · · · · · · · · · · ·		SUB-	TRANSLATION	
	REF	NUMBER	DATE		COUNTRY	CLASS	CLASS	YES	NO
<del></del>							<u> </u>		
		-					1		
	L	OTHER DOCU	MENTS (Includir	ng Auti	nor, Title, Date,	Pertinent Pages,	Etc.)	i	
	OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)  All Gligor Virgil D. and Donescu Pompiliu. "Fast Encryption and Authentication: XCBC Encryption and XECB Authentication Modes." VDG Inc. 27 October 2000. Pages 1 – 30. <a href="http://citeseer.nj.nec.com/cs">http://citeseer.nj.nec.com/cs</a> .								
1									lessage
M	A2	Rogaway, Phillip. "Comments to NIST Concerning AES Modes of Operation: PMAC: A Parallelizable Message Authentication Code." Univ. of CA at Davis and Chiang Mai Univ. Thailand. 16 October 2000. Pages 1 – 6. http://citeseer.nj.nec.com/cs>.							
n	А3	Proceedings IEEE Symposium on Security and Privacy. Jueneman, R.R., Matyas, S.M., and Meyer, C.H. "Message Authentication with Manipulation Detection Codes." Pages 33 – 54. 25 April 1983.							
,		:							
EXAMINER	L		·····		DATE CONSID	DERED	<del></del>		
$\mathcal{M}$				/2	-17/04				
EXAMINER: Initial if citation considered, whether				hether			nce with M	IPEP 609	); Draw
	_	n citation if not in tion to applicant.	conformance	and n	ot considered.	include any c	opy of this	form wi	th next